



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/829,674

04/10/2001

Katsuaki Akama

FUJA 18.570

1585

26304

7590

11/10/2005

KATTEN MUCHIN ROSENMAN LLP  
575 MADISON AVENUE  
NEW YORK, NY 10022-2585

EXAMINER

PYZOCHA, MICHAEL J

ART UNIT

PAPER NUMBER

2137

DATE MAILED: 11/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.



**DETAILED ACTION**

1. Claims 1-10 are pending.
2. Amendment filed 02/23/2005 has been received and considered.

***Claim Rejections - 35 USC § 112***

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 1-6 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.
5. In claim 1 the phrase "public/secret keys" is unclear, because the "/" could and, or, and/or. For the purpose of examination it will be assumed the "/" means or.
6. Any claims not specifically addressed are rejected by virtue of their dependencies.

***Claim Rejections - 35 USC § 103***

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rowney (US 6373950) and further in view of Menezes et al (Handbook of Applied Cryptography).

As per claim 10, Rowney a user terminal being able to communicate with a first server and a second server (see Fig. 1B); and wherein the first sever includes a proxy facility for executing authentication with the second server instead of the user terminal when receiving an identification information and a request for executing an authentication process from the user terminal (see column 14, lines 46-51); and the second server has an authentication facility to authenticate the user terminal in accordance with predetermined procedures and to provide a secret key for an authorized destination as a result of authentication (see column 19, lines 25-35); and wherein the user terminal comprises a transmitting unit to transmit the identification

Art Unit: 2137

information used for identifying its own terminal and the request for executing the authentication process, to the first server, and a receiving unit to receive the secret information from the first server (see column 20, lines 7-17). The payment gateway computer is considered a part of the proxy server system.

Rowney fails to disclose the common key is encrypted using another common key.

However, Menezes teaches such keys (see pages 15 and 552).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use a common key and to encrypt the common key.

Motivation to do so would have been to allow for high rates of data throughput (see page 31) and to transport or store the key (see page 552).

9. Claims 1-2, 4-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rowney (US 6373950), further in view of Baskey et al (US 6732269) and further in view of Menezes et al (Handbook of Applied Cryptography).

As per claim 1, Rowney discloses a user terminal and an electronic market server where authentication and encryption is used between the two (see column 4 lines 43-55), establishing means for establishing an encrypted communication session

Art Unit: 2137

between the user terminal and the proxy server, using public and secret keys of the user terminal and an electronic signature both transmitted from the user terminal on column 14, lines 46-67 and on column 15, lines 1-5; and a proxy means for executing authentication of a certificate and exchanging a key between the proxy server and the electronic market server, using public/secret keys of the electronic market server on column 19, lines 25-43; and an information means for informing the key to the user terminal through the encrypted communication session and wherein an encrypted communication is executed between the user terminal and the electronic market server by using the key that was exchanged between the proxy server and the electronic market server" on column 14, lines 35-40 and 55-61. The customer computer system represents the user terminal. The merchant computer system represents the proxy server and the host legacy system in combination with the payment gateway system represent the proxy. The electronic signature is inherently present on the exchanged certificates. The payment gateway computer system is considered a part of the proxy/legacy server system because it provides reformatting functions that aid further functions of the proxy/legacy system towards authentication. It would have been obvious to one of ordinary skill in the art at the time of the invention to have the host

Art Unit: 2137

legacy system in combination with the payment gateway system represent the proxy because they both work together towards the authentication of the client.

Rowney fails to disclose the proxy server being provided between a user terminal and an electronic market server and the shared key being a common key, which is encrypted using another common key.

However, Baskey et al teaches a proxy server between a client and a server (see column 5 lines 17-37) and Menezes teaches a common key and encrypting the key (see pages 15 and 552).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Baskey's proxy server between the client and merchant and for the client and merchant to use Menezes' common key and to encrypt the common key in Rowney's security method.

Motivation to do so would have been to provide scalable secure communications (see column 5 lines 17-37) and to allow for high rates of data throughput (see page 31) and to transport or store the key (see page 552).

With respect to Claim 2, the limitation of "a proxy card including an encryption managing means for executing the electronic signature and authentication of the certificate in

Art Unit: 2137

order to execute authentication and exchange of the common key to the electronic market server" is met on column 2, lines 35-38 and on column 15, lines 47-58. The smart card inherently has an encryption managing means that performs authorization, key exchange and electronic signature execution.

With respect to Claim 4, the limitation of "wherein the proxy card comprises an information means for recording decision information regarding an electronic money in the proxy card and for informing the recorded decision information to a mail address of the user terminal" is met on column 108, lines 8-9, 13-15. The memory of the smart card makes the existence of an information means for recording decision information inherent in the reference.

With respect to Claim 5, the limitation of "wherein the proxy card comprises a cancel means for canceling the decision information in the proxy card based on an authentication information for canceling the decision, and for adding electronic money subtracted by the decision to the electronic money in the proxy card" is met on column 107, lines 45-57. The cancel means would have been obvious to one of ordinary skill in the art at the time of the invention because the electronic wallet in the reference has an interface that allows for reading and writing of information to itself. Because electronic money



Art Unit: 2137

can be subtracted from the electronic wallet, so also would it be obvious to add electronic money to the wallet due to a canceled transaction/decision or simply just to transfer one's balance onto the wallet from a pre-existing account.

With respect to Claim 6, the limitation of "wherein the proxy card comprises a re-supplement means for supplementing the electronic money by adding supplementary electronic money, which was requested by the user terminal, to the electronic money in the proxy card, based on the authentication information in an electronic money managing facility provided in the proxy facility" is met inherently on column 107, lines 6 1-65 and on column 108, lines 16-22. Visa and debit cards are inherently forms of supplemental electronic money.

With respect to Claim 7, the limitation of "a proxy server and an electronic market server; the access card being connected to the user terminal; and the proxy server including a proxy facility being provided between the user terminal and the electronic market server for executing authentication and encryption to the electronic market server, instead of the user terminal; the access card" is met on column 4, lines 43-55 and on column 108, lines 7-22; and "an establishment means for establishing an encrypted communication session between the user terminal and the proxy server including the proxy facility" is

Art Unit: 2137

met on column 14, lines 66-67 and on column 15, lines 1-8; and "an encrypted communication means for receiving a common key, which is exchanged between the proxy server and the electronic market server after an authentication process for the electronic market server, from the proxy server through the encrypted communication session, and for executing the encrypted communication with the electronic market server by using the common key" is met on column 19, lines 25-35 with the encrypted common key as applied above.

With respect to Claim 8, the limitation of "a reception unit to receive an identification information and a request for executing an authentication process, from the user terminal and a decision means for determining whether or not the identification information is stored in an internal or external memory" is met on column 14, lines 47-51, 55-61. The decision means is inherent from the fact that the merchant verifies the client's certificate. Further limitation of "a proxy means for executing a part, or all, communication in accordance with the predetermined procedures when the identification information is stored in the memory" is met on column 17, lines 45-49, 59-67 and on column 18, lines 1-4 with the encrypted common key as applied above.

With respect to Claim 9, its limitation is similar to Claim 8 limitation and hence its rejection can be found therein.

10. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Rowney, Baskey and Menezes system and further in view of Mooney et al (US 6351813).

With respect to Claim 3, the modified Rowney, Baskey and Menezes system meets all the limitation except for the following limitation. The limitation of "wherein the proxy card includes a logic circuit which enables an access by using a first password input from the user terminal; and a security releasing means for releasing the security for the proxy means by using a second password input from the user terminal, after establishment of the encrypted communication session to the user terminal in which an access was permitted" is met by Mooney et al on column 1, lines 59-67, column 2, lines 1- 11 and on column 9, lines 31-36.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Mooney et al within the system of Rowney because a smart card and password combination system as a means of authentication is a well-known method of authentication in the art.

***Response to Arguments***

11. Applicant's arguments with respect to claims 1-10 have been considered but are moot in view of the new ground(s) of rejection.

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2137

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJP

*Matthew B. Smithers*  
MATTHEW SMITHERS  
PRIMARY EXAMINER  
*Art Unit 2137*